REMARKS/ARGUMENTS

The Applicant has amended the claims to clarify that which the Applicant considers to be the invention. The Applicant respectfully submits that amendments to the claim set are fully supported by the originally filed specification.

Independent claims 1 and 6 have been amended to limit the claims to applying a first key from the trusted authentication chip to produce a first encrypted outcome, and using a second key from the untrusted authentication chip to produce a second encrypted outcome. The first encrypted outcome and the second encrypted outcome are then compared without knowledge of the first key or the second key. This is supported by reference to Fig. 3 and the associated description from page 36, line 22 – page 39, line 2.

The amendments to dependent claims 2, 5, 7 and 12 are for clarity purposes to refer to first and second keys.

In relation to the double patenting rejection a terminal disclaimer is filed in compliance with 37 CFR 1.321(c).

At pages 4-7 of the Office Action, the Examiner rejects claims 1-4, 6, 7, 11 and 12 under 35 USC 102(b) as being anticipated by Abraham *et al.* (US 4,799,061).

In the presently claimed invention a "first encrypted outcome" is obtained by applying a keyed one way function to the random number using a first key. The "second encrypted outcome" is obtained by applying a keyed one way function to the random number using a second key. The presently claimed invention then compares "the first encrypted outcome and the second encrypted outcome, without knowledge of the first key or the second key".

This does not occur in Abraham. Referring to Fig. 2 and col. 3, lines 4-46 of Abraham, two embodiments are disclosed. In the first embodiment, the decrypted value of Z, obtained using the random number as a key, at step 38, is compared to key K1. Importantly, such a comparison requires knowledge of key K1. The presently claimed invention explicitly recites that knowledge of the first key or the second key is not required. Furthermore, the comparison in Abraham is between the key K1 and a decrypted function which uses the random number RN as a decryption key. In contrast, in the presently claimed invention, the comparison is between outcomes performed on the random number, not using the random number itself as a key.

In the second embodiment disclosed in Abraham, the comparison is between two values A and B, obtained at steps 38 and 38a respectively, which are values obtained by using the random number RN as a decryption and encryption key. The random number RN is used as a decryption/encryption key and applied to the values Z and the key K1. This is the opposite of what is claimed in the presently claimed invention, whereby the "first encrypted outcome" and the "second encrypted outcome" are obtained by applying a first key and a second key respectively to the random number, not using the random number as the key itself. Also, at step 38a, to be able to apply an encryption function to key K1 knowledge of key K1 is required. The pres ntly claimed invention explictly states that the comparison is made "without knowledge of the first key or the second key".

For at least the aforementioned reasons, it is respectfully submitted that independent claims 1 and 6 of the present application are not anticipated by or obvious in light of Abraham *et al.*, or other prior art documents of record. Likewise, the dependent claims of the present application are respectfully submitted to be patentable over Abraham *et al.* or Thomlinson *et al.*, for the 35 USC 103(a) rejection against claims 5 and 8-10, when taken individually or in combination with any of the other prior art documents of record.

CONCLUSION

In view of the foregoing, it is respectfully requested that the Examiner reconsider and withdraw the rejections under 35 USC 102(b) and 35 USC 103(a). The present application is believed to be in condition for allowance. Accordingly, the Applicant respectfully requests a Notice of Allowance of all the claims presently under examination.

Very respectfully,

Applicant:

SIMON ROBERT WALMSLEY

PAUL LAPSTUN

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762